SAE INTERNATIONAL

SAE J3061™ “CYBERSECURITY GUIDEBOOK FOR CYBER-PHYSICAL VEHICLE SYSTEMS”

AGENDA

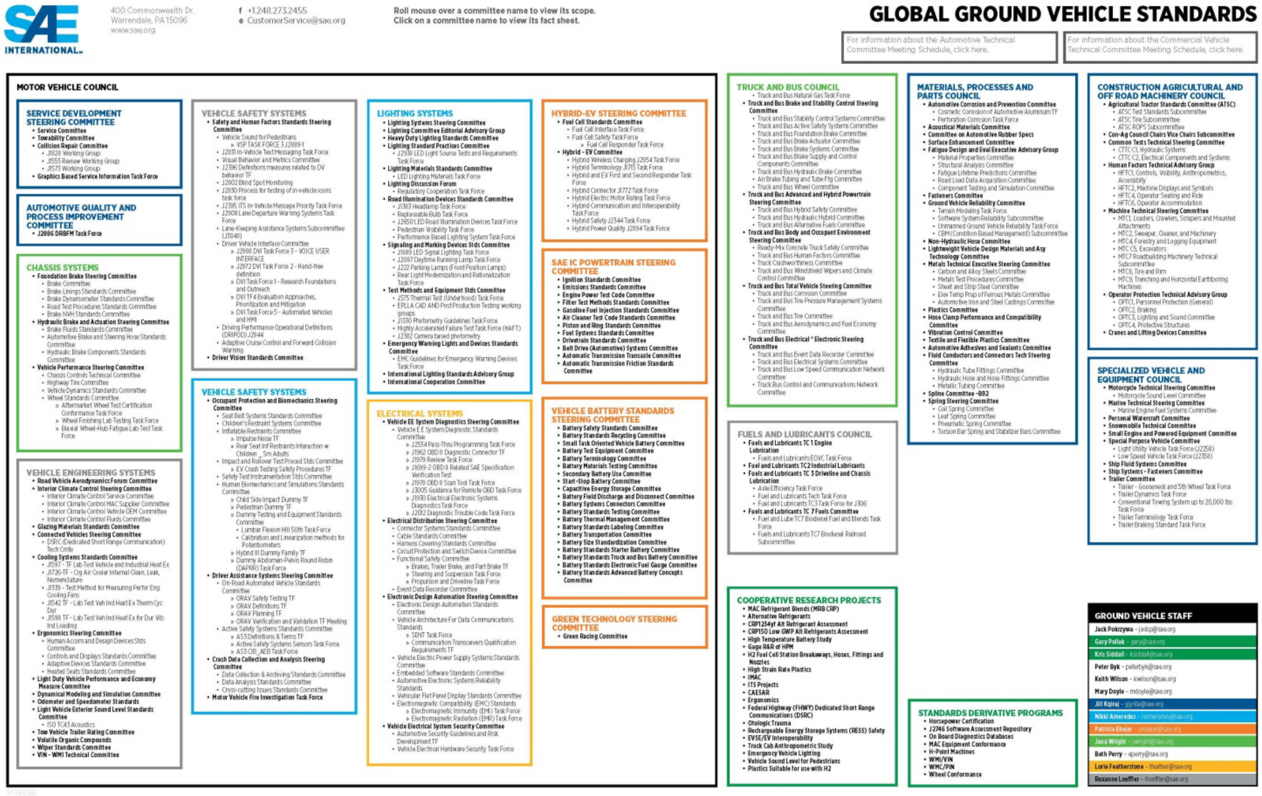
Introduction

SAE Vehicle Electrical System Security Committee

Overview of SAE J3061™

J3061™ webinar on December 3

SAE Standards Development



SAE INTERNATIONAL

400 Commonwealth Dr.
Warrendale, PA 15096
www.sae.org

t +1.248.273.2455
e CustomerService@sae.org

Roll mouse over a committee name to view its scope.
Click on a committee name to view its fact sheet.

GLOBAL GROUND VEHICLE STANDARDS

For information about the Automotive Technical Committee Meeting Schedule, click here.

For information about the Commercial Vehicle Technical Committee Meeting Schedule, click here.

MOTOR VEHICLE COUNCIL

SERVICE DEVELOPMENT STEERING COMMITTEE
- **Service Committee**
- **Towability Committee**
- **Collision Repair Committee**
  - J1828 Working Group
  - J1555 Review Working Group
  - J1573 Working Group
- **Graphics Based Service Information Task Force**

AUTOMOTIVE QUALITY AND PROCESS IMPROVEMENT COMMITTEE
- **J2886 DRBFM Task Force**

CHASSIS SYSTEMS
- **Foundation Brake Steering Committee**
  - Brake Committee
  - Brake Linings Standards Committee
  - Brake Dynamometer Standards Committee
  - Road Test Procedures Standards Committee
  - Brake NVH Standards Committee
- **Hydraulic Brake and Actuation Steering Committee**
  - Brake Fluids Standards Committee
  - Automotive Brake and Steering Hose Standards Committee
  - Hydraulic Brake Components Standards Committee
- **Vehicle Performance Steering Committee**
  - Chassis Controls Technical Committee
  - Highway Tire Committee
  - Vehicle Dynamics Standards Committee
  - Wheel Standards Committee
    - Aftermarket Wheel Test Certification Conformance Task Force
    - Wheel Finishing Lab Testing Task Force
    - Biaxial Wheel-Hub Fatigue Lab Test Task Force

VEHICLE ENGINEERING SYSTEMS
- **Road Vehicle Aerodynamics Forum Committee**
- **Interior Climate Control Steering Committee**
  - Interior Climate Control Service Committee
  - Interior Climate Control MAC Supplier Committee
  - Interior Climate Control Vehicle OEM Committee
  - Interior Climate Control Fluids Committee
- **Glazing Materials Standards Committee**
- **Connected Vehicles Steering Committee**
  - DSRC (Dedicated Short Range Communication) Tech Cmte
- **Cooling Systems Standards Committee**
  - J1597 - TF Lab Test Vehicle and Industrial Heat Ex
  - J1726-TF - Crg Air Cooler Internal Clean, Leak, Nomenclature
  - J1339 - Test Method for Measuring Perfor Eng Cooling Fans
  - J1542 TF - Lab Test Veh Ind Heat Ex Therm Cyc Dur
  - J1598 TF - Lab Test Veh Ind Heat Ex for Dur Vib Ind Loading
- **Ergonomics Steering Committee**
  - Human Accom and Design Devices Stds Committee
  - Controls and Displays Standards Committee
  - Adaptive Devices Standards Committee
  - Heated Seats Standards Committee
- **Light Duty Vehicle Performance and Economy Measure Committee**
- **Dynamical Modeling and Simulation Committee**
- **Odometer and Speedometer Standards**
- **Light Vehicle Exterior Sound Level Standards Committee**
  - ISO TC43 Acoustics
- **Tow Vehicle Trailer Rating Committee**
- **Volatile Organic Compounds**
- **Wiper Standards Committee**
- **VIN - WMI Technical Committee**

VEHICLE SAFETY SYSTEMS
- **Safety and Human Factors Standards Steering Committee**
  - Vehicle Sound for Pedestrians
    - VSP TASK FORCE 3 J2889-1
  - J2831 In-Vehicle Text Messaging Task Force
  - Visual Behavior and Metrics Committee
  - J2396 Definitions measures related to DV behavior TF
  - J2802 Blind Spot Monitoring
  - J2830 Process for testing of in-vehicle icons task force
  - J2395 ITS In-Vehicle Message Priority Task Force
  - J2808 Lane Departure Warning Systems Task Force
  - Lane-Keeping Assistance Systems Subcommittee (J3048)
  - Driver Vehicle Interface Committee
    - J2988 DVI Task Force 3 - VOICE USER INTERFACE
    - J2972 DVI Task Force 2 - Hand-free definition
    - DVI Task Force 1 - Research Foundations and Outreach
    - DVI TF4 Evaluation Approaches, Prioritization and Mitigation
    - DVI Task Force 5 - Automated Vehicles and HMI
  - Driving Performance Operational Definitions (DRIPOD) J2944
  - Adaptive Cruise Control and Forward Collision Warning
- **Driver Vision Standards Committee**

VEHICLE SAFETY SYSTEMS
- **Occupant Protection and Biomechanics Steering Committee**
  - Seat Belt Systems Standards Committee
  - Children's Restraint Systems Committee
  - Inflatable Restraints Committee
    - Impulse Noise TF
    - Rear Seat Inf Restraints Interaction w Children _ Sm Adults
  - Impact and Rollover Test Proced Stds Committee
    - EV Crash Testing Safety Procedures TF
  - Safety Test Instrumentation Stds Committee
  - Human Biomechanics and Simulations Standards Committee
    - Child Side Impact Dummy TF
    - Pedestrian Dummy TF
    - Dummy Testing and Equipment Standards Committee
      - Lumbar Flexion HIII 50th Task Force
      - Calibration and Linearization methods for Potentiometers
    - Hybrid III Dummy Family TF
    - Dummy Abdomen-Pelvis Round Robin (DAPRR) Task Force
- **Driver Assistance Systems Steering Committee**
  - On-Road Automated Vehicle Standards Committee
    - ORAV Safety Testing TF
    - ORAV Definitions TF
    - ORAV Planning TF
    - ORAV Verification and Validation TF Meeting
  - Active Safety Systems Standards Committee
    - AS3 Definitions & Terms TF
    - Active Safety Systems Sensors Task Force
    - AS3 CIB_AEB Task Force
- **Crash Data Collection and Analysis Steering Committee**
  - Data Collection & Archiving Standards Committee
  - Data Analysis Standards Committee
  - Cross-cutting Issues Standards Committee
- **Motor Vehicle Fire Investigation Task Force**

LIGHTING SYSTEMS
- **Lighting Systems Steering Committee**
- **Lighting Committee Editorial Advisory Group**
- **Heavy Duty Lighting Standards Committee**
- **Lighting Standard Practices Committee**
  - J2938 LED Light Source Tests and Requirements Task Force
- **Lighting Materials Standards Committee**
  - LED Lighting Materials Task Force
- **Lighting Discussion Forum**
  - Regulatory Cooperation Task Force
- **Road Illumination Devices Standards Committee**
  - J1383 Headlamp Task Force
  - Replaceable Bulb Task Force
  - J2650 LED Road Illumination Devices Task Force
  - Pedestrian Visibility Task Force
  - Performance Based Lighting System Task Force
- **Signaling and Marking Devices Stds Committee**
  - J1889 LED Signal Lighting Task Force
  - J2087 Daytime Running Lamp Task Force
  - J222 Parking Lamps (Front Position Lamps)
  - Rear Light Modernization and Rationalization Task Force
- **Test Methods and Equipment Stds Committee**
  - J575 Thermal Test (Underhood) Task Force
  - EPLLA CAD AND Post Production Testing working groups
  - J1330 Photometry Guidelines Task Force
  - Highly Accelerated Failure Test Task Force (HAFT)
  - J2382 Camera based photometry
- **Emergency Warning Lights and Devices Standards Committee**
  - EMC Guidelines for Emergency Warning Devices Task Force
- **International Lighting Standards Advisory Group**
- **International Cooperation Committee**

ELECTRICAL SYSTEMS
- **Vehicle EE System Diagnostics Steering Committee**
  - Vehicle E E System Diagnostic Standards Committee
    - J2534 Pass-Thru Programming Task Force
    - J1962 OBD II Diagnostic Connector TF
    - J1979 Review Task Force
    - J1699-2 OBD II Related SAE Specification Verification Test
    - J1978 OBD II Scan Tool Task Force
    - J3005 Guidance for Remote OBD Task Force
    - J1930 Electrical Electronic Systems Diagnostics Task Force
    - J2012 Diagnostic Trouble Code Task Force
- **Electrical Distribution Steering Committee**
  - Connector Systems Standards Committee
  - Cable Standards Committee
  - Harness Covering Standards Committee
  - Circuit Protection and Switch Device Committee
  - Functional Safety Committee
    - Brakes, Trailer Brake, and Part Brake TF
    - Steering and Suspension Task Force
    - Propulsion and Driveline Task Force
  - Event Data Recorder Committee
- **Electronic Design Automation Steering Committee**
  - Electronic Design Automation Standards Committee
  - Vehicle Architecture For Data Communications Standards
    - SENT Task Force
    - Communication Transceivers Qualification Requirements TF
  - Vehicle Electric Power Supply Systems Standards Committee
  - Embedded Software Standards Committee
  - Automotive Electronic Systems Reliability Standards
  - Vehicular Flat Panel Display Standards Committee
  - Electromagnetic Compatibility (EMC) Standards
    - Electromagnetic Immunity (EMI) Task Force
    - Electromagnetic Radiation (EMR) Task Force
- **Vehicle Electrical System Security Committee**
  - Automotive Security Guidelines and Risk Development TF
  - Vehicle Electrical Hardware Security Task Force

HYBRID-EV STEERING COMMITTEE
- **Fuel Cell Standards Committee**
  - Fuel Cell Interface Task Force
  - Fuel Cell Safety Task Force
    - Fuel Cell Responder Task Force
- **Hybrid - EV Committee**
  - Hybrid Wireless Charging J2954 Task Force
  - Hybrid Terminology J1715 Task Force
  - Hybrid and EV First and Second Responder Task Force
  - Hybrid Connector J1772 Task Force
  - Hybrid Electric Motor Rating Task Force
  - Hybrid Communication and Interoperability Task Force
  - Hybrid Safety J2344 Task Force
  - Hybrid Power Quality J2894 Task Force

SAE IC POWERTRAIN STEERING COMMITTEE
- **Ignition Standards Committee**
- **Emissions Standards Committee**
- **Engine Power Test Code Committee**
- **Filter Test Methods Standards Committee**
- **Gasoline Fuel Injection Standards Committee**
- **Air Cleaner Test Code Standards Committee**
- **Piston and Ring Standards Committee**
- **Fuel Systems Standards Committee**
- **Drivetrain Standards Committee**
- **Belt Drive (Automotive) Systems Committee**
- **Automatic Transmission Transaxle Committee**
- **Automatic Transmission Friction Standards Committee**

VEHICLE BATTERY STANDARDS STEERING COMMITTEE
- **Battery Safety Standards Committee**
- **Battery Standards Recycling Committee**
- **Small Task Oriented Vehicle Battery Committee**
- **Battery Test Equipment Committee**
- **Battery Terminology Committee**
- **Battery Materials Testing Committee**
- **Secondary Battery Use Committee**
- **Start-Stop Battery Committee**
- **Capacitive Energy Storage Committee**
- **Battery Field Discharge and Disconnect Committee**
- **Battery Systems Connectors Committee**
- **Battery Standards Testing Committee**
- **Battery Thermal Management Committee**
- **Battery Standards Labeling Committee**
- **Battery Transportation Committee**
- **Battery Size Standardization Committee**
- **Battery Standards Starter Battery Committee**
- **Battery Standards Truck and Bus Battery Committee**
- **Battery Standards Electronic Fuel Gauge Committee**
- **Battery Standards Advanced Battery Concepts Committee**

GREEN TECHNOLOGY STEERING COMMITTEE
- **Green Racing Committee**

P136558

TRUCK AND BUS COUNCIL
  - Truck and Bus Natural Gas Task Force
- **Truck and Bus Brake and Stability Control Steering Committee**
  - Truck and Bus Stability Control Systems Committee
  - Truck and Bus Active Safety Systems Committee
  - Truck and Bus Foundation Brake Committee
  - Truck and Bus Brake Actuator Committee
  - Truck and Bus Brake Systems Committee
  - Truck and Bus Brake Supply and Control Components Committee
  - Truck and Bus Hydraulic Brake Committee
  - Air Brake Tubing and Tube Ftg Committee
  - Truck and Bus Wheel Committee
- **Truck and Bus Advanced and Hybrid Powertrain Steering Committee**
  - Truck and Bus Hybrid Safety Committee
  - Truck and Bus Hydraulic Hybrid Committee
  - Truck and Bus Alternative Fuels Committee
- **Truck and Bus Body and Occupant Environment Steering Committee**
  - Ready-Mix Concrete Truck Safety Committee
  - Truck and Bus Human Factors Committee
  - Truck Crashworthiness Committee
  - Truck and Bus Windshield Wipers and Climate Control Committee
- **Truck and Bus Total Vehicle Steering Committee**
  - Truck and Bus Corrosion Committee
  - Truck and Bus Tire Pressure Management Systems Committee
  - Truck and Bus Tire Committee
  - Truck and Bus Aerodynamics and Fuel Economy Committee
- **Truck and Bus Electrical * Electronic Steering Committee**
  - Truck and Bus Event Data Recorder Committee
  - Truck and Bus Electrical Systems Committee
  - Truck and Bus Low Speed Communication Network Committee
  - Truck Bus Control and Communications Network Committee

FUELS AND LUBRICANTS COUNCIL
- **Fuels and Lubricants TC 1 Engine Lubrication**
  - Fuels and Lubricants EOVC Task Force
- **Fuel and Lubricants TC2 Industrial Lubricants**
- **Fuels and Lubricants TC 3 Driveline and Chassis Lubrication**
  - Axle Efficiency Task Force
  - Fuel and Lubricants Tech Task Force
  - Fuel and Lubricants TC3 Task Force for J306
- **Fuels and Lubricants TC 7 Fuels Committee**
  - Fuel and Lube TC7 Biodiesel Fuel and Blends Task Force
  - Fuels and Lubricants TC7 Biodiesel Railroad Subcommittee

COOPERATIVE RESEARCH PROJECTS
- **MAC Refrigerant Blends (MRB CRP)**
- **Alternative Refrigerants**
- **CRP1234yf Alt Refrigerant Assessment**
- **CRP150 Low GWP Alt Refrigerants Assessment**
- **High Temperature Battery Study**
- **Gage R&R of HPM**
- **H2 Fuel Cell Station Breakaways, Hoses, Fittings and Nozzles**
- **High Strain Rate Plastics**
- **IMAC**
- **ITS Projects**
- **CAESAR**
- **Ergonomics**
- **Federal Highway (FHWY) Dedicated Short Range Communications (DSRC)**
- **Otologic Trauma**
- **Rechargeable Energy Storage Systems (RESS) Safety**
- **EVSE/EV Interoperability**
- **Truck Cab Anthropometric Study**
- **Emergency Vehicle Lighting**
- **Vehicle Sound Level for Pedestrians**
- **Plastics Suitable for use with H2**

MATERIALS, PROCESSES AND PARTS COUNCIL
- **Automotive Corrosion and Prevention Committee**
  - Cosmetic Corrosion of Automotive Aluminum TF
  - Perforation Corrosion Task Force
- **Acoustical Materials Committee**
- **Committee on Automotive Rubber Specs**
- **Surface Enhancement Committee**
- **Fatigue Design and Eval Executive Advisory Group**
  - Material Properties Committee
  - Structural Analysis Committee
  - Fatigue Lifetime Predictions Committee
  - Road Load Data Acquisition Committee
  - Component Testing and Simulation Committee
- **Fasteners Committee**
- **Ground Vehicle Reliability Committee**
  - Terrain Modeling Task Force
  - Software System Reliability Subcommittee
  - Unmanned Ground Vehicle Reliability Task Force
  - CBM (Condition Based Management) Subcommittee
- **Non-Hydraulic Hose Committee**
- **Lightweight Vehicle Design Materials and Asy Technology Committee**
- **Metals Technical Executive Steering Committee**
  - Carbon and Alloy Steels Committee
  - Metals Test Procedures Committee
  - Sheet and Strip Steel Committee
  - Elev Temp Prop of Ferrous Metals Committee
  - Automotive Iron and Steel Castings Committee
- **Plastics Committee**
- **Hose Clamp Performance and Compatibility Committee**
- **Vibration Control Committee**
- **Textile and Flexible Plastics Committee**
- **Automotive Adhesives and Sealants Committee**
- **Fluid Conductors and Connectors Tech Steering Committee**
  - Hydraulic Tube Fittings Committee
  - Hydraulic Hose and Hose Fittings Committee
  - Metallic Tubing Committee
- **Spline Committee -B92**
- **Spring Steering Committee**
  - Coil Spring Committee
  - Leaf Spring Committee
  - Pneumatic Spring Committee
  - Torsion Bar Spring and Stabilizer Bars Committee

STANDARDS DERIVATIVE PROGRAMS
- **Horsepower Certification**
- **J2746 Software Assessment Repository**
- **On Board Diagnostics Databases**
- **MAC Equipment Conformance**
- **H-Point Machines**
- **WMI/VIN**
- **WMC/PIN**
- **Wheel Conformance**

CONSTRUCTION AGRICULTURAL AND OFF ROAD MACHINERY COUNCIL
- **Agricultural Tractor Standards Committee (ATSC)**
  - ATSC Test Standards Subcommittee
  - ATSC Tire Subcommittee
  - ATSC ROPS Subcommittee
- **Con-Ag Council Chairs Vice Chairs Subcommittee**
- **Common Tests Technical Steering Committee**
  - CTTC C1, Hydraulic Systems
  - CTTC C2, Electrical Components and Systems
- **Human Factors Technical Advisory Group**
  - HFTC1, Controls, Visibility, Anthropometrics, Accessiblity
  - HFTC2, Machine Displays and Symbols
  - HFTC4, Operator Seating and Ride
  - HFTC6, Operator Accommodation
- **Machine Technical Steering Committee**
  - MTC1, Loaders, Crawlers, Scrapers and Mounted Attachments
  - MTC2, Sweeper, Cleaner, and Machinery
  - MTC4, Forestry and Logging Equipment
  - MTC C5, Excavators
  - MTC7 Roadbuilding Machinery Technical Subcommittee
  - MTC8, Tire and Rim
  - MTC9, Trenching and Horizontal Earthboring Machines
- **Operator Protection Technical Advisory Group**
  - OPTC1, Personnel Protection (General)
  - OPTC2, Braking
  - OPTC3, Lighting and Sound Committee
  - OPTC4, Protective Structures
- **Cranes and Lifting Devices Committee**

SPECIALIZED VEHICLE AND EQUIPMENT COUNCIL
- **Motorcycle Technical Steering Committee**
  - Motorcycle Sound Level Committee
- **Marine Technical Steering Committee**
  - Marine Engine Fuel Systems Committee
- **Personal Watercraft Committee**
- **Snowmobile Technical Committee**
- **Small Engine and Powered Equipment Committee**
- **Special Purpose Vehicle Committee**
  - Light Utility Vehicle Task Force (J2258)
  - Low Speed Vehicle Task Force (J2358)
- **Ship Fluid Systems Committee**
- **Ship Systems - Fasteners Committee**
- **Trailer Committee**
  - Trailer - Gooseneck and 5th Wheel Task Force
  - Trailer Dynamics Task Force
  - Conventional Towing System up to 20,000 lbs Task Force
  - Trailer Terminology Task Force
  - Trailer Braking Standard Task Force

GROUND VEHICLE STAFF

Jack Pokrzywa - jackp@sae.org
Gary Pollak - gary@sae.org
Kris Siddall - ksiddall@sae.org
Peter Byk - peterbyk@sae.org
Keith Wilson - kwilson@sae.org
Mary Doyle - mdoyle@sae.org
Jill Kqiraj - gjysta@sae.org
Nikki Ameredes - nameredes@sae.org
Patricia Ebejer - pebejer@sae.org
Jana Wright - jwright@sae.org
Beth Perry - eperry@sae.org
Lorie Featherstone - lfeather@sae.org
Roxanne Loeffler - rloeffler@sae.org

609 committees

8,865 members

2,898 companies

1,423 meetings

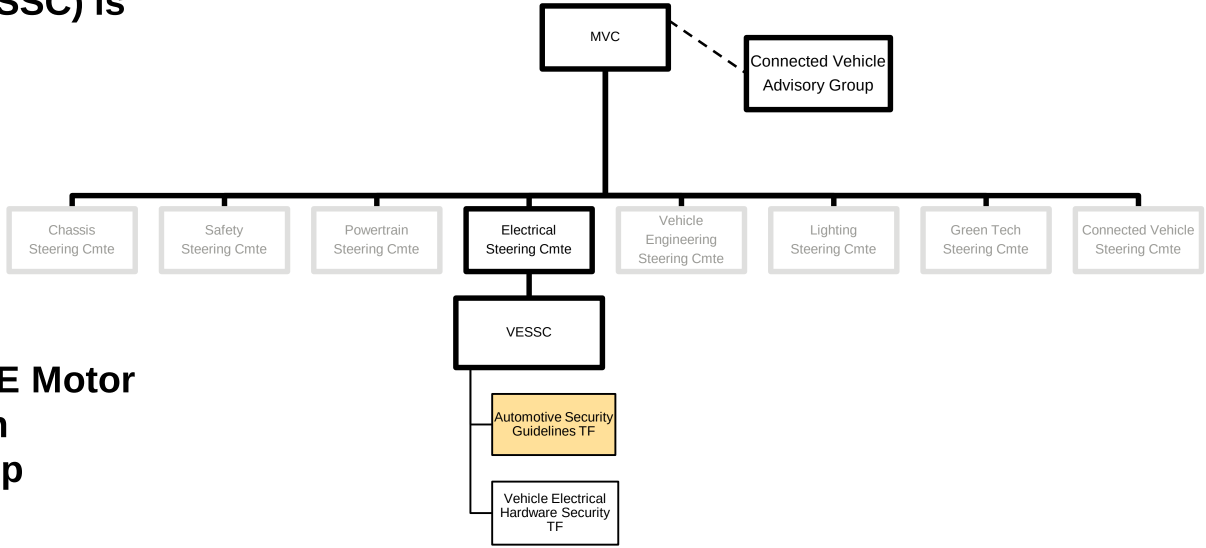
Committee meetings are open to all interested parties, but only committee members vote on draft documents.

Individuals participate on committees as technical experts and not as representatives of their organizations

SAE Vehicle Electrical System Security Committee (VESSC)

- The Vehicle Electrical System Security Committee (VESSC) is active since May 5, 2011

- Organized under the SAE Motor Vehicle Council (MVC) in Electrical Systems Group


MVC
Connected Vehicle Advisory Group
Chassis Steering Cmte
Safety Steering Cmte
Powertrain Steering Cmte
Electrical Steering Cmte
Vehicle Engineering Steering Cmte
Lighting Steering Cmte
Green Tech Steering Cmte
Connected Vehicle Steering Cmte
VESSC
Automotive Security Guidelines TF
Vehicle Electrical Hardware Security TF

Technology background*

- About 50% of car manufacturing cost is in electronics

- Global data collection from connected cars could rise to 545 petabytes by 2020 up from 345 terabytes in 2013**

- OTA enabled vehicle sales per year will likely rise to 26.7 million in 2020 from 2.6 million in 2014

- Global sales of connected passenger vehicles projected to grow to 77 million units annually by 2022 from about 19 million in 2014 - 73% of vehicles sold will be connected in some way.

- Space shuttle - 500k lines of code
- Boeing 777 - 3-4 million lines of code
- Ford Taurus 2012 - 50+ million lines of code
- Today cars - 100 millions lines of code

** Various forecast sources* *** petabyte=1 million gigabytes, terabyte=1,000 gigabytes)*

Committee charter

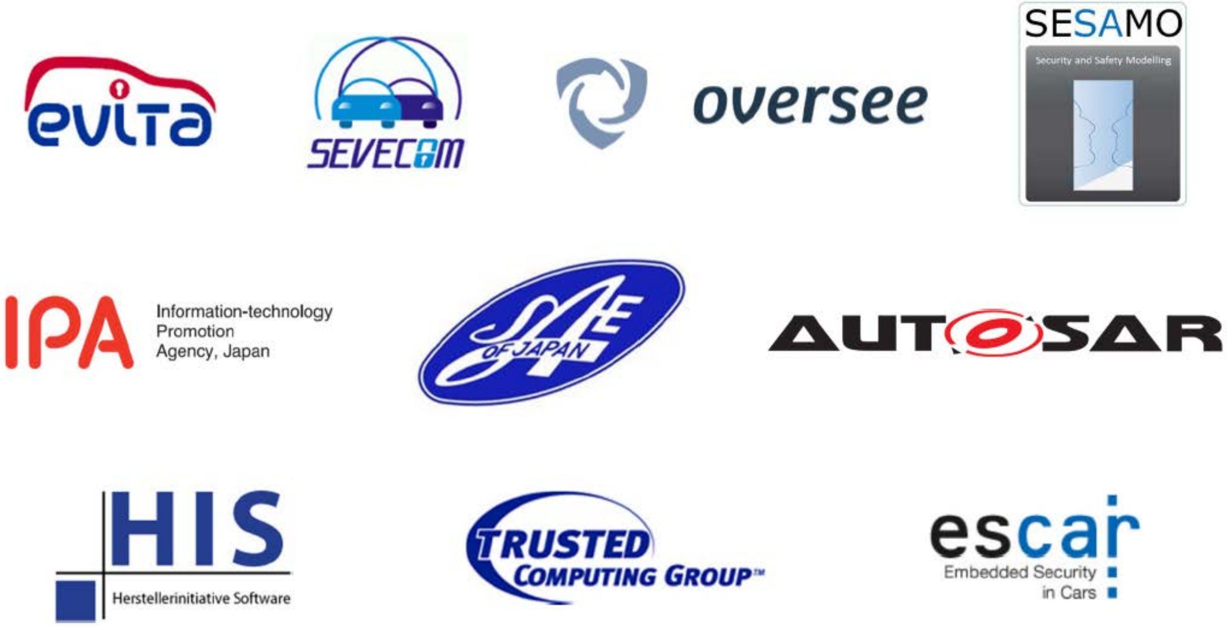
“The SAE Vehicle Electrical System Security Committee is responsible for developing and maintaining Recommended Practices and Information Reports in the area of vehicle electrical systems’ security. The committee’s scope is on-board vehicle electrical systems that affect vehicle control or otherwise act contrary to the occupants’ interests if the systems are manipulated by an attacker. The goals of the committee are:

- To identify and recommend strategies and techniques related to preventing and detecting adversarial breaches, and
- Mitigating undesirable effects if a breach is achieved.

The group will classify attack methods, propose preventative strategies, define levels of security by criticality of system type, and identify architecture-level strategies for mitigating attacks. Participants in the Committee include OEMs, suppliers, consulting firms, government entities, and other interested parties.”

Interaction with other activities

Other Activities



J3061™ – What is it?

This recommended practice establishes a set of high-level guiding principles for *cybersecurity* as it relates to automotive *cyber-physical systems* to be utilized in series production. This includes:

- Defining a framework for a lifecycle process to incorporate cybersecurity into automotive cyber-physical systems.
- Providing information on some common tools and methods used when designing and validating *cyber-physical automotive systems.*
- Providing basic Guiding Principles on Cybersecurity for Automotive Systems.
- Providing the foundation for further standards development activities in vehicle cybersecurity.

J3061™ – When to apply

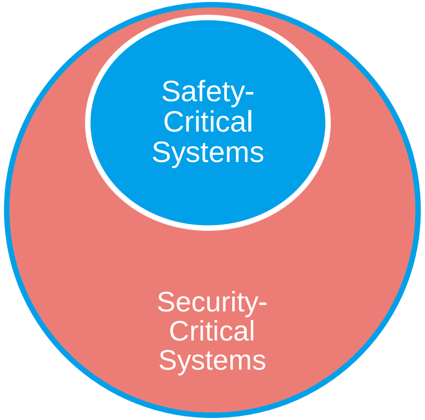
- J3061™ recommends that a cybersecurity process be applied for all automotive systems that are responsible for functions that are ASIL (Automotive Safety Integrity Level) rated per ISO 26262, or that are responsible for functions associated with:
  - Propulsion
  - Braking
  - Steering
  - Security
  - Safety

- J3061™ also recommends that a cybersecurity process be applied for automotive systems that handle *Personally Identifiable Information (PII)*.

- For other systems that may also be considered cybersecurity-critical cyber-physical automotive systems, an initial short assessment of threats and an initial estimate of risks can be made to determine if the system being considered should follow a cybersecurity process.

J3061™ – System Safety vs System Cybersecurity

- System safety is the state of a system that does not cause harm to life, property, or the environment.
  - A safety-critical system is a system that may cause harm to life, property, or the environment if the system does not behave as intended or desired
- System cybersecurity is the state of a system that does not allow exploitation of vulnerabilities to lead to losses, such as financial, operational, privacy, or safety losses
  - A security-critical system is a system that may lead to financial, operational, privacy, or safety losses if the system is compromised through a vulnerability that may exist in the system
- All safety-critical systems are security-critical since a cyber-attack either directly or indirectly on a safety-critical system could lead to potential safety losses
- Not all security-critical systems are safety-critical, i.e. entertainment system
- Some systems are both, safety and security critical, i.e. Steering Assist System



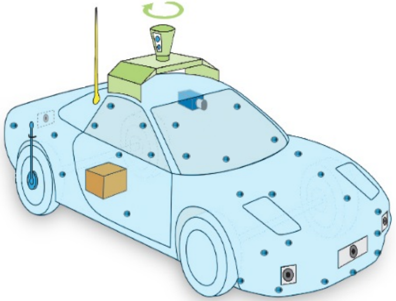
J3061™ – System Safety vs System Cybersecurity

- System Safety considers potential hazards to identify safety mechanisms that can be integrated into the design to address the causes of the potential hazards
  - Potential hazards and causes are more readily identified
  - Appropriate action to mitigate the potential consequences, or to eliminate the potential hazards all together can be taken
  - Causes of hazards based knowledge of system, components, and interactions
  - Focus on sub-systems
- System cybersecurity considers potential threats posed by a malicious attacker whose goal is to cause harm, wreak havoc, gain financial benefits, or simply to gain notoriety
  - Cyber Security threats are more difficult to address than potential safety hazards
  - More difficult to try to anticipate the exact moves an attacker may take in order to add appropriate Security Controls to protect against attacker's options.
  - Causes maybe unknown
  - Additional factors in risk assessment: attacker's experience level, attacker's access, attacker's need for special equipment
  - Focus on sub-systems AND electrical architecture (i.e. possible access to safety-critical areas through non-safety-critical area, i.e. CD player)

J3061™ – System Safety vs System Cybersecurity

- Cybersecurity is not concerned with random hardware failures, but it is concerned with systematic hardware vulnerabilities

- Goals are the same – analysis methods may be different:
  - System Safety may utilize detailed hazard analysis technique *Fault Tree Analysis (FTA)*
    - Fault Tree Analysis identifies potential causes of the top hazard event and looks for single-point and multi-point random hardware failures.
  - System cybersecurity may utilize detailed threat analysis technique *Attack Tree Analysis (ATA)*.
    - Attack Tree Analysis we are not concerned with single-point and multi-point random hardware failures, but rather with determining potential paths that an attacker could take through the system to lead to the top level threat.



J3061™ – Guiding Principles

- Know Your System's Cybersecurity Risks
  - Will there be any Sensitive data and/or Personally Identifiable Information (PII) stored on, or transmitted by, your system?
  - What role does your system have (if any) in the safety critical functions of a vehicle?
  - What communications or connections will your system have with entities that are external to the vehicle's electrical architecture?
  - Conduct the appropriate Risk/Threat Analysis

- Understand Key Cybersecurity Principles
  - Protect Personally identifiable information (PII) and Sensitive data
  - Use the principle of "Least Privilege" -- All components run with the fewest possible permissions.
  - Apply "Defense in Depth", particularly for the highest risk threats
  - Prohibit risky changes to calibrations and/or software.
  - Vehicle-Level: Prevent users from making unauthorized changes that could reduce security for the vehicle after it has been sold. Some potential violations of this principle include:
    - "Tuners", Software that may come from a DVD, Bluetooth-paired phone, etc.

J3061™ – Guiding Principles

- Consider Vehicle Owners’ Use of System
  - Minimize data collection
  - Enable user policy and control.
  - Protect the storage, usage, and transfer of PII data
  - Provide appropriate notice about data that is collected, stored, or shared

- Implement Cybersecurity in Concept and Design Phases
  - The system should be defined with cybersecurity in mind, starting in the concept phase of the development lifecycle.
  - Analyze threats (i.e., initiated external or internal to the system, and often of malicious intent) to determine what risks and attack surfaces will be faced by the system.
  - Implement cybersecurity analysis and management tools that enable engineers to determine and configure the optimal security level for the system.

J3061™ – Guiding Principles

- Implement Cybersecurity in Development & Validation
  - Review design to assess whether the cybersecurity requirements are being met.
  - Conduct testing to confirm that the requirements that were established for cybersecurity at the beginning of the design phase have been met in the modules/controllers/*ECUs* and in the overall vehicle design.
  - Test software patch/revision deployment tools and processes to ensure that any approved re-flashes to the vehicle software can be done without adversely affecting the vehicle's cybersecurity defenses.

- Implement Cybersecurity in Incident Response
  - Revise (or create) the Incident Response Process so that it comprehends cybersecurity incidents
  - Publish deployment guides
  - Determine how software and/or calibration updates will be made if there is an incident
  - Vehicle-Level: Develop appropriate material for dealerships, customer assistance help lines, websites, and owner's manuals.

- Cybersecurity Considerations at End of Life
  - Determine whether there are any ECUs on the vehicle that need to have SW/HW or Customer Personal Information that needs to be erased to protect the customer, or protect the organization (e.g. immobilizer, cell phone pairing).
  - Provide a method to remove personal information off the vehicle or module upon change of ownership and/or end of vehicle life..

J3061™ – Cybersecurity Process Overview

Management of cybersecurity consists of two aspects:

1. **The overall management of cybersecurity Part of the overall management of cybersecurity includes:**
   - Creating, fostering, and sustaining a cybersecurity culture within the organization,
   - Establishing methods to help ensure compliance to an adopted cybersecurity engineering process,
   - Identifying and establishing needed communication channels with respect to cybersecurity, both internally and externally,
   - Development and implementation of training and mentoring
   - Incorporating an expanded field monitoring process that includes monitoring ***hacker chatter*** (including online and at conferences where potential attacks/vulnerability conversations may occur), reporting unsuccessful attacks, etc., and
   - Incorporating an incident response process is important and should include an attack incident reporting procedure, and attack incident investigation, resolution, and action procedures.

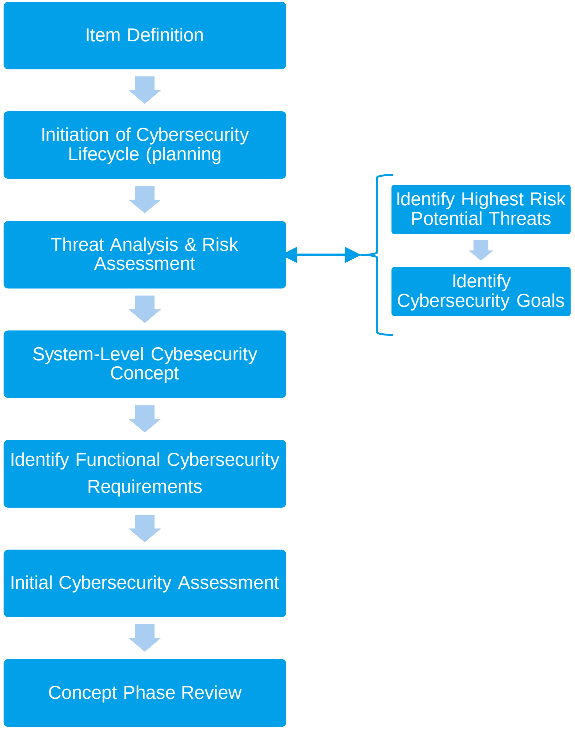
2. **Management of cybersecurity activities within specific stages of the development life cycle.**

J3061™ – Cybersecurity Process Overview

Concept Phase

The initiation of the cybersecurity lifecycle includes development of the Cybersecurity Program Plan that describes the activities to be carried out as part of the cybersecurity lifecycle.

The *Threat Analysis and Risk Assessment (TARA)* activity is used to assess the potential threats to the system and to determine the risk associated with each of the threats.


Item Definition
Initiation of Cybersecurity Lifecycle (planning
Threat Analysis & Risk Assessment
System-Level Cybesecurity Concept
Identify Functional Cybersecurity Requirements
Initial Cybersecurity Assessment
Concept Phase Review
Identify Highest Risk Potential Threats
Identify Cybersecurity Goals

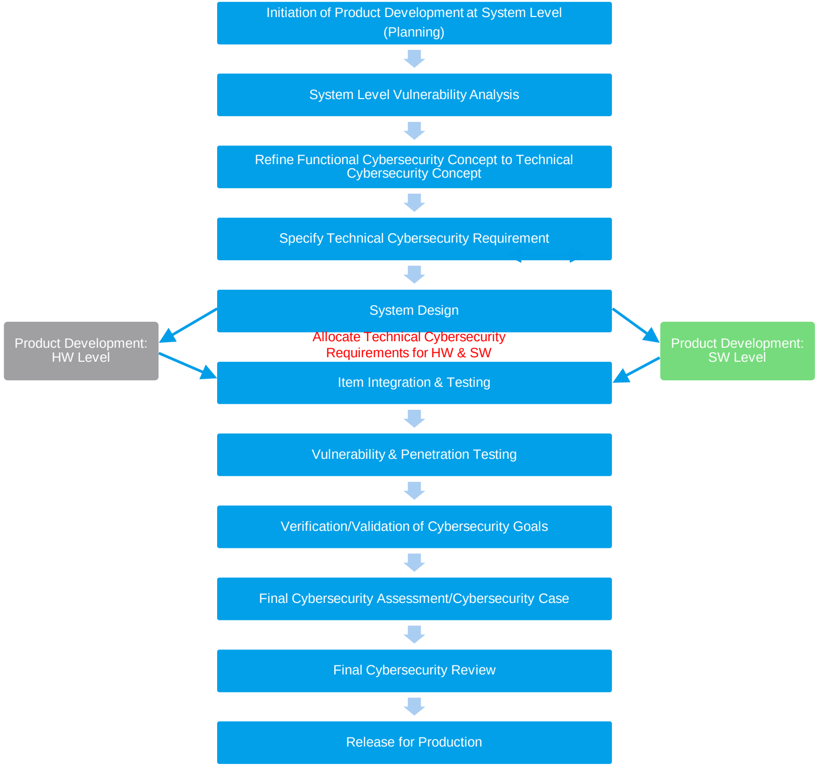
J3061™ – Cybersecurity Process Overview

Product Development: Systems Level

A System Context is created to define the interfaces between the system's hardware and software, the key data flows, storage and processing within the system.

Using the System Context, the system-level technical cybersecurity requirements are then allocated to hardware and software or to both.

Once the technical cybersecurity requirements have been allocated to hardware and/or software, the activities at the Product Development: Hardware Level and Product Development: Software Level can begin


Initiation of Product Development at System Level (Planning)
System Level Vulnerability Analysis
Refine Functional Cybersecurity Concept to Technical Cybersecurity Concept
Specify Technical Cybersecurity Requirement
System Design
Product Development: HW Level
Product Development: SW Level
Allocate Technical Cybersecurity Requirements for HW & SW
Item Integration & Testing
Vulnerability & Penetration Testing
Verification/Validation of Cybersecurity Goals
Final Cybersecurity Assessment/Cybersecurity Case
Final Cybersecurity Review
Release for Production

J3061™ – Cybersecurity Process Overview

Product Development: Hardware Level

Hardware security requirements would be specified from the cybersecurity requirements allocated to hardware during the system level development.

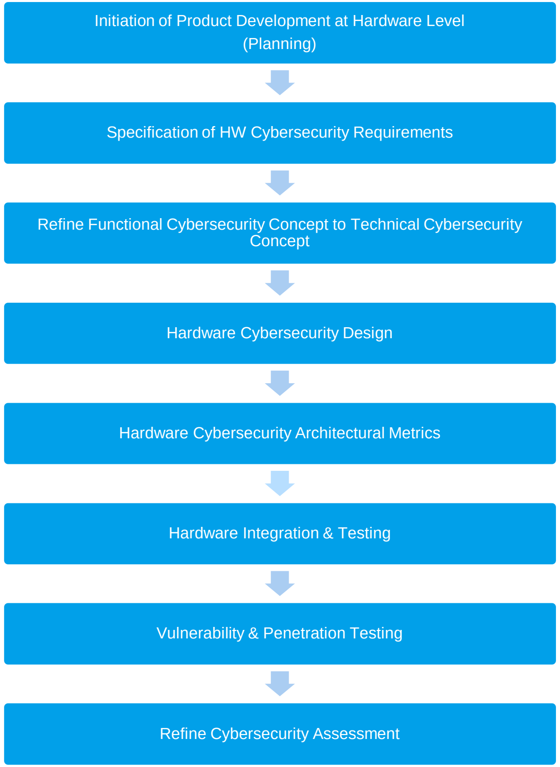
If applicable, the Technical Security Concept could be refined at this stage.

Following hardware design, a vulnerability analysis would be performed to help identify potential vulnerabilities in the design and to help identify potential Security Controls to address the potential vulnerabilities.

If there are appropriate hardware security architectural metrics, these would be identified.

Following hardware integration and testing, vulnerability and penetration testing may be applied to the hardware design.

A cybersecurity assessment is then performed and the preliminary cybersecurity assessment is refined



Initiation of Product Development at Hardware Level (Planning)

Specification of HW Cybersecurity Requirements

Refine Functional Cybersecurity Concept to Technical Cybersecurity Concept

Hardware Cybersecurity Design

Hardware Cybersecurity Architectural Metrics

Hardware Integration & Testing

Vulnerability & Penetration Testing

Refine Cybersecurity Assessment

J3061™ – Cybersecurity Process Overview

Product Development: Software Level

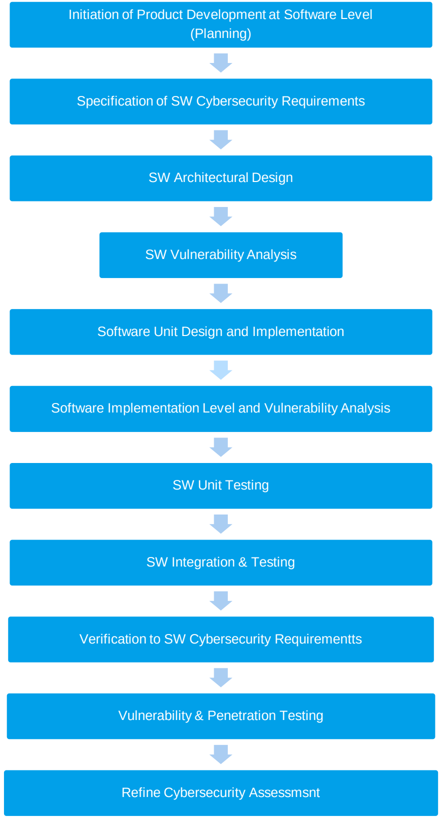
Software security requirements would be specified from the cybersecurity requirements allocated to software during the system level development.

If applicable, the Technical Security Concept could be refined at this stage.

Following software architectural design, a vulnerability analysis would be performed to help identify potential vulnerabilities in the software architectural design and to help identify potential Security Controls to address the potential vulnerabilities.

Following software unit design and implementation, a software level vulnerability analysis may be performed, followed by software unit testing and software integration and testing.

The software cybersecurity requirements are verified after software integration, and vulnerability and penetration testing may be performed on the software. A cybersecurity assessment is then performed and the previous cybersecurity assessment is refined



Initiation of Product Development at Software Level (Planning)

Specification of SW Cybersecurity Requirements

SW Architectural Design

SW Vulnerability Analysis

Software Unit Design and Implementation

Software Implementation Level and Vulnerability Analysis

SW Unit Testing

SW Integration & Testing

Verification to SW Cybersecurity Requirementts

Vulnerability & Penetration Testing

Refine Cybersecurity Assessmsnt

J3061™ – Cybersecurity Process Overview

Production and Operation/Service

The operation phase includes:

- Operation - Any requirements specific to cybersecurity during operation, should be recorded within the appropriate documents (e.g., Vehicle Owner's Operating Manual).
- Service
  - Normal maintenance activities
  - Repair

Maintenance and repair activities that could affect cybersecurity should have been identified in earlier lifecycle phases

Service that could affect cybersecurity includes re-flashing ECU's, connecting to the on-board diagnostics port, telematics system updates, vehicle/cloud computing interfaces, etc.

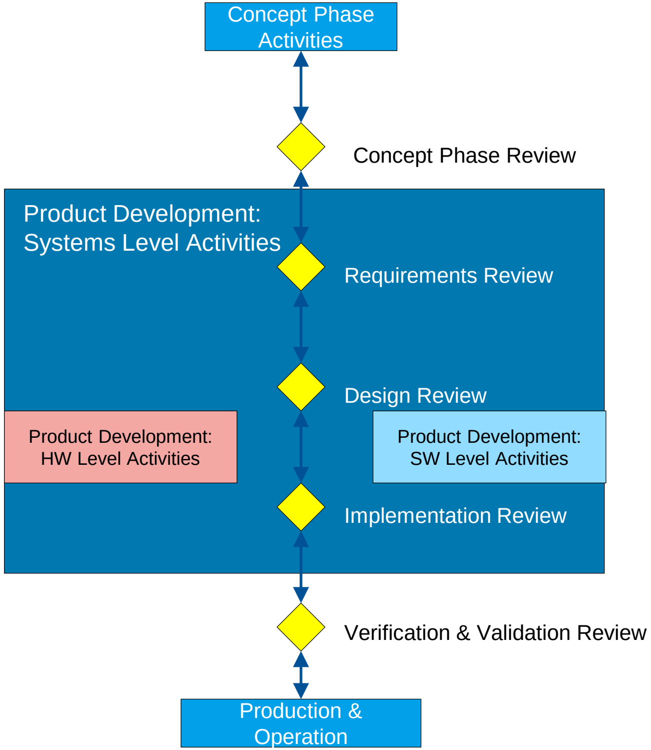
Supporting Processes - configuration management, documentation management, change management, management of cybersecurity requirements, requirements for dealing with distributed development should ensure that:

- supplier is capable of developing and producing cybersecurity-critical features according to a customer organizations internal cybersecurity process,
- appropriate communication channels are established and maintained between the supplier and customer,
- cybersecurity work products are agreed to,
- appropriate reviews are established at key milestones with customer access to work products,
- changes that could affect cybersecurity are evaluated and agreed to,
- final cybersecurity case is reviewed and agreed to,
- cybersecurity issues that the supplier may become aware of are reported to the customer in a timely manner, etc.

J3061™ – Cybersecurity Process Overview

Gate reviews

- The gate reviews are intended to help ensure that appropriate activities have been performed and completed correctly and consistently before the next stage of development begins.
- These reviews may be conducted by a small (e.g., 3-4 person) team of technical experts that should ideally be independent of the feature development.
- To maintain consistency and completeness across the feature development, it is recommended that this same 3-4 person team participates in all of the reviews throughout the system development.
- The results of each review may be a pass, or a conditional pass (rework required).
- A gate review should be completed successfully prior to exiting the gate and moving on to the next phase.


Concept Phase Activities
Concept Phase Review
Product Development: Systems Level Activities
Requirements Review
Design Review
Product Development: HW Level Activities
Product Development: SW Level Activities
Implementation Review
Verification & Validation Review
Production & Operation

J3061™ – Overall Management of Cybersecurity

J3061™ provides detailed recommendation on each of the concepts below:

- Creating, fostering, and sustaining a cybersecurity culture that supports and encourages effective achievement of cybersecurity within the organization,
- Establishing methods to help ensure compliance to an adopted cybersecurity engineering process,
- Identifying and establishing needed communication channels with respect to cybersecurity, both internally and externally,
- Development and implementation of training and mentoring to achieve a competence in cybersecurity for cyber-physical vehicle systems,
- Incorporating a field monitoring process that includes monitoring hacker chatter (including online and at conferences where potential attacks/vulnerability conversations may occur), media articles, reporting unsuccessful attacks, etc.,
- Incorporating an incident response process that includes an attack incident reporting procedure, and attack incident investigation, resolution, and action procedures.

J3061™ – Process Implementation

Three types of implementation:

1. Applying a Cybersecurity Process Separately with Integrated Communication Points to a Safety Process
   - Some advantages to this approach are that though the two domains (cybersecurity and safety) have analogous activities from a process perspective, the activities are different and can impact different domains (e.g., cybersecurity often impacts infotainment, which is typically a domain not impacted by safety), and require different types of expertise
2. Applying a Cybersecurity Process in Conjunction with a Safety Process Tailored after ISO 26262
   - Since the cybersecurity process described in this recommended practice is based on the ISO 26262 process framework, tightly integrating the two processes would simply mean to include the cybersecurity activities described in this document for each product lifecycle phase, with the corresponding activities for each product lifecycle phase described in the safety process.
3. Some cybersecurity processes and steps are shared with safety and some that are unique to cybersecurity only.

It is up to the organization to make decision on which is most suitable.

J3061™ explains in detail each approach focusing on concept, product development, production operation and service in software and hardware design

J3061™ Appendix A – Description of Cybersecurity Analysis Techniques

J3061™ appendix A outlines a sampling of security analysis techniques including the methods used by:

- E-Safety Vehicle Intrusion Protected Applications (EVITA) program
- Threat, Vulnerabilities, and implementation Risks Analysis (TVRA) method
- Operationally Critical Threat, Asset, and Vulnerability Evaluation (OCTAVE) method
- HEAling Vulnerabilities to ENhance Software Security and Safety (HEAVENS) method and attack tree information

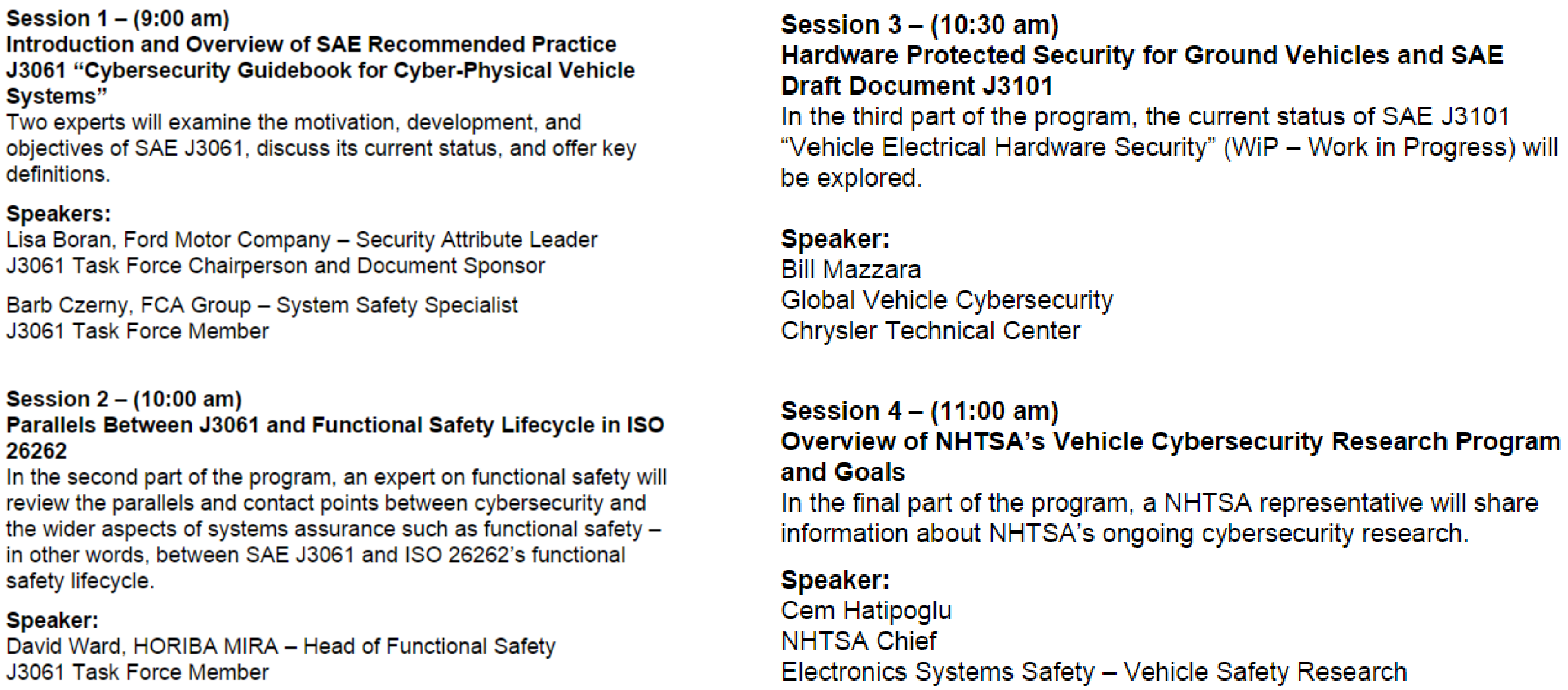
J3061™ Appendix B – Example templates For Work Products

- In J3061™ Appendix B several examples of a template for an OCTAVE worksheet are provided.

- Appendix B does not give examples of the other methods described in Appendix A, and the Recommended Practice does not, at this time, recommend specific methods.

- Therefore, it is up to each organization to determine whether to use one of the methods described Appendix A or whether to use a different method

You are welcome to attend a webinar on SAE J3061™ "Cybersecurity Guidebook for Cyber-Physical Vehicle Systems"



Session 1 – (9:00 am)
Introduction and Overview of SAE Recommended Practice J3061 "Cybersecurity Guidebook for Cyber-Physical Vehicle Systems"
Two experts will examine the motivation, development, and objectives of SAE J3061, discuss its current status, and offer key definitions.

Speakers:
Lisa Boran, Ford Motor Company – Security Attribute Leader
J3061 Task Force Chairperson and Document Sponsor

Barb Czerny, FCA Group – System Safety Specialist
J3061 Task Force Member

Session 2 – (10:00 am)
Parallels Between J3061 and Functional Safety Lifecycle in ISO 26262
In the second part of the program, an expert on functional safety will review the parallels and contact points between cybersecurity and the wider aspects of systems assurance such as functional safety – in other words, between SAE J3061 and ISO 26262's functional safety lifecycle.

Speaker:
David Ward, HORIBA MIRA – Head of Functional Safety
J3061 Task Force Member

Session 3 – (10:30 am)
Hardware Protected Security for Ground Vehicles and SAE Draft Document J3101
In the third part of the program, the current status of SAE J3101 "Vehicle Electrical Hardware Security" (WiP – Work in Progress) will be explored.

Speaker:
Bill Mazzara
Global Vehicle Cybersecurity
Chrysler Technical Center

Session 4 – (11:00 am)
Overview of NHTSA's Vehicle Cybersecurity Research Program and Goals
In the final part of the program, a NHTSA representative will share information about NHTSA's ongoing cybersecurity research.

Speaker:
Cem Hatipoglu
NHTSA Chief
Electronics Systems Safety – Vehicle Safety Research

https://event.webcasts.com/starthere.jsp?ei=1080592

You are welcome to attend a webinar on SAE J3061™ "Cybersecurity Guidebook for Cyber-Physical Vehicle Systems"

https://event.webcasts.com/starthere.jsp?ei=1080592

The event will be recorded for future on-demand viewing

What’s next

- J3061™ team is discussing potential joint work with ISO counterpart to develop one global standard based on J3061™
- SAE is developing training program around J3061™ for automotive companies
- J3101 – new standard “Vehicle Electrical Hardware Security” is being developed

Contact

Jack Pokrzywa
Director
SAE Global Ground Vehicle Standards
US TAG ISO TC22 Chairperson

SAE INTERNATIONAL
755 West Big Beaver Road, Suite 1600
Troy, MI 48084

o +1.248.273.2460
m +1.248.219.2412
e jack.pokrzywa@sae.org
www.sae.org